(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Patentschrift**

(10) **DE 197 44 293 C 1**

(51) Int. Cl.[6]:
H 04 L 9/32
H 04 N 7/16
H 04 N 7/173

(21) Aktenzeichen: 197 44 293.5-31
(22) Anmeldetag: 7. 10. 97
(43) Offenlegungstag: –
(45) Veröffentlichungstag der Patenterteilung: 1. 7. 99

Innerhalb von 3 Monaten nach Veröffentlichung der Erteilung kann Einspruch erhoben werden

(73) Patentinhaber:
Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V., 80636 München, DE

(74) Vertreter:
Schoppe, F., Dipl.-Ing.Univ., Pat.-Anw., 81479 München

(61) Zusatz zu: 196 25 635.6

(72) Erfinder:
Rump, Niels, Dipl.-Inform., 91056 Erlangen, DE;
Sieler, Martin, Dipl.-Ing., 91207 Lauf, DE

(56) Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:

US 53 69 702
US 53 19 705

(54) Verschlüsselung und Entschlüsselung von Multimediadaten

(57) Ein Verfahren zum Verschlüsseln von Multimediadaten weist das Eintragen eines Verschlüsselungsindex in einen Bestimmungsdatenblock der Multimediadaten auf, der auf einen zu verwendenden Verschlüsselungsalgorithmus hinweist. Als Reaktion auf den Verschlüsselungsindex in dem Bestimmungsdatenblock wird ein Verschlüsselungsalgorithmus aus einer Mehrzahl von Verschlüsselungsalgorithmen ausgewählt. Unter Verwendung des ausgewählten Verschlüsselungsalgorithmus werden die Multimediadaten verschlüsselt. Verschiedene weitere Einträge in dem Bestimmungsdatenblock, der den Multimediadaten zugeordnet wird, erlauben eine Freischaltung einer Entschlüsselungsvorrichtung, einen schnellen Zugriff auf eine Datenbank von verschlüsselten Multimediadaten sowie eine Kunden- und datenspezifische Benutzung der Multimediadaten unter Berücksichtigung urheberrechtlicher Gesichtspunkte. Die verschlüsselten Multimediadaten werden in ein Haupt-Bestimmungsdatenpaket, ein Multimediadaten-Bestimmungsdatenpaket und ein Multimediadatenpaket verpackt, um eine Übertragung bzw. Speicherung in einer fehlerbehafteten Umgebung zu ermöglichen.

DE 197 44 293 C 1

DE 197 44 293 C 1

Beschreibung

Die vorliegende Erfindung bezieht sich auf die Verschlüsselung und Entschlüsselung von Multimediadaten und insbesondere auf Vorrichtungen und Verfahren zum Verschlüsseln und Entschlüsseln von Multimediadaten gemäß dem Hauptpatent 19625635.6-31.

Mit dem Auftreten von Telekommunikationsnetzen und insbesondere aufgrund der großen Verbreitung von Multimediadaten-fähigen Personalcomputern entstand ein Bedarf, digitale Multimediadaten, wie z. B. digitale Audiodaten oder digitale Videodaten, kommerziell zu vertreiben. Die Telekommunikationsnetze können beispielsweise analoge Telefonleitungen, digitale Telefonleitungen, wie z. B. ISDN, oder auch das Internet sein. Unter kommerziellen Anbietern von Multimediaprodukten besteht der Bedarf, Multimediadaten zu verkaufen oder auszuleihen, wobei es einem Kunden möglich sein sollte, aus einem bestimmten Katalog zu jeder Zeit individuell ein bestimmtes Produkt auswählen zu können, das dann selbstverständlich nur von dem Kunden, der dafür bezahlt, benutzt werden kann.

Im Gegensatz zu bekannten verschlüsselten Fernsehprogrammen, wie z. B. den Fernsehkanälen Premiere oder MTV, bei denen die ausgesendeten Daten für alle Benutzer, die gegen eine bestimmte Gebühr eine geeignete Entschlüsselungsvorrichtung erworben haben, gleich verschlüsselt ist, schafft die vorliegende Erfindung Verfahren und Vorrichtungen, die eine individuelle, kundenselektive Verschlüsselung und Entschlüsselung von Multimediadaten ermöglichen. Im Gegensatz zu den genannten Fernsehkanälen, die ein festes Programm vorgeben, für das sich der Benutzer komplett entscheiden muß, ermöglichen die Verfahren und Vorrichtungen der vorliegenden Erfindung eine maximale Wahlfreiheit des Kunden, d. h. derselbe muß nur für die Produkte bezahlen, die er tatsächlich auch benutzt hat.

Das U. S. Patent Nr. 5,369,702 offenbart ein System zum Erhöhen der Sicherheit eines Computersystems, wobei einzelne Benutzer dasselbe flexibel und effizient nützen können. Das in dieser Schrift offenbarte Verfahren umfaßt die Schritte des Zugreifens auf einen objektorientierten Schlüsselverwalter, des Auswählens eines zu verschlüsselnden Objekts, des Auswählens einer Etikette für das Objekt, des Auswählens eines Verschlüsselungsalgorithmus, des Verschlüsselns des Objekts gemäß dem Verschlüsselungsalgorithmus, des Etikettierens des verschlüsselten Objekts, des Lesens des Objektetiketts, des Bestimmens einer Zugriffsermächtigung basierend auf dem Objektetikett und des Entschlüsselns des Objekts, wenn die Zugriffsermächtigung erteilt ist. Eine Datei-"Etikette" besteht aus einer Serie von Buchstaben oder Zahlen, welche verschlüsselt oder nicht verschlüsselt sein können.

Das U. S. Patent Nr. 5,319,705 betrifft ein Verfahren und ein System zum sicheren Verteilen einer Mehrzahl von Softwaredateien von einem Softwareverteilsprozessor zu einem Benutzerprozessor, während der Benutzerprozessor selektiv in die Lage versetzt wird, nur eine Teilmenge einer kleineren Mehrzahl von Softwaredateien zu verwenden. Dies wird durch Verwenden eines Kundenschlüssels erreicht, welcher einen unverschlüsselten Kundenschlüssel und einen abgeleiteten Abschnitt aufweist, der aus der Kundennummer abgeleitet ist.

Die Aufgabe der Erfindung nach dem Hauptpatent besteht darin, Verfahren und Vorrichtungen zum Verschlüsseln und Entschlüsseln von Multimediadaten zu schaffen, welche zum einen einen wirksamen Urheberrechtsschutz garantieren und zum anderen in der Lage sind, individuell angeforderte Daten zu ver- bzw. entschlüsseln.

Der Erfindung gemäß dem Hauptpatent liegt die Erkenntnis zugrunde, daß ein ausreichender Urheberrechtsschutz für Audio- und Videoprodukte, welche in Form von digitalen Multimediadaten vorliegen, nur dann gewährleistet werden kann, wenn möglichst unmittelbar nach der Produktion der digitalen Multimediadaten, die beispielsweise gemäß dem bekannten Standard MPEG Audio Layer 3 codiert bzw. komprimiert sind, eine sichere Verschlüsselung durchgeführt wird. Für Fachleute ist es offensichtlich, daß die Erfindung gemäß dem Hauptpatent nicht auf die Verwendung von Daten in dem Format MPEG Layer 3 begrenzt ist, sondern daß auch unkomprimierte Multimediadaten oder nach irgendeinem anderen Verfahren komprimierte Multimediadaten ebenfalls verwendet werden können.

Nachdem die Multimediadaten vor ihrer Speicherung/Lagerung von einer Verschlüsselungsvorrichtung verschlüsselt worden sind, können sie individuell von einem Benutzer angefordert werden, der sich im Besitz einer geeigneten Entschlüsselungsvorrichtung befindet. Diese Entschlüsselungsvorrichtung darf jedoch nur zur Durchführung ihrer Aufgaben den Verschlüsselungsschutz um die Daten herum lösen, wobei ebenfalls von großer Bedeutung ist, daß nicht jede Entschlüsselungsvorrichtung in der Lage ist, die Multimediadaten zu lesen, sondern nur die Entschlüsselungsvorrichtung, die sich bei dem Kunden befindet, der für die Multimediadaten bezahlt hat. Ferner ist es wichtig, daß es dem Benutzer möglichst schwer wenn nicht unmöglich gemacht wird, die Multimediadaten selbst sowie die Verschlüsselung unerlaubt zu verändern.

Sollte ein Benutzer versuchen, die Multimediadaten zu verändern, dann ist es wünschenswert, daß die Daten vollständig unlesbar sind. Die Tatsache, daß die Verschlüsselungsvorrichtung bereits an ihrem Ausgang verschlüsselte Dateien erzeugt, den Schutz gewissermaßen sofort über die Multimediadaten legt, gewährleistet also, daß keine ungeschützten Daten am Beginn einer Übertragungs/Speicherungs-Kette auftreten.

Die Entschlüsselungsvorrichtung ist in der Lage, die speziell verschlüsselten Daten zu lesen. Das Verfahren zum Verschlüsseln von Multimediadaten gemäß der Erfindung des Hauptpatents erzeugt zusätzlich zu vorliegenden unverschlüsselten Multimediadaten einen Bestimmungsdatenblock, in dem sich verschiedene Informationen bezüglich der Verschlüsselung der unverschlüsselten Multimediadaten sowie bezüglich allgemeiner und spezieller Funktionen, die von der Erfindung des Hauptpatents ausgeführt werden können, befinden.

Einige der Funktionalitäten, die von einer Entschlüsselungsvorrichtung gemäß der Erfindung des Hauptpatents gefordert werden, werden nachfolgend beschrieben:

Eine Entschlüsselungsvorrichtung der Erfindung des Hauptpatents soll in der Lage sein, einen Demoabspieler für Audiodaten in dem Format ISO MPEG Layer 3 zu implementieren, welcher es nur zuläßt, daß etwa die ersten 20 Sekunden einer Audioaufzeichnung abgespielt werden. Unter bestimmten Umständen soll es nun möglich sein, daß der Demoabspieler bei einem bestimmten Kunden bestimmte Musikstücke länger als 20 Sekunden abspielt. Dies wird durch eine sogenannte Freischaltung des Bitstroms erreicht, welche durch bestimmte in dem Bestimmungsdatenblock vorhandene Einträge bewirkt wird.

Weiterhin soll die Erfindung gemäß dem Hauptpatent in der Lage sein, eine Entschlüsselungsvorrichtung, d. h. einen Abspieler, für Audiodaten im Format MPEG Layer 3 zu implementieren, der es nur bestimmten Kunden erlaubt, eine bestimmte Audiodatei abzuspielen. Dies dient zum Urheberrechtsschutz für Audio- bzw. Videowerke, wobei ein Abspielen lediglich nach Bezahlung einer Gebühr möglich sein soll.

Zusätzlich soll die Erfindung gemäß dem Hauptpatent einen Spieler implementieren, der nicht nur den Inhalt einer Audiodatendatei abspielen kann, sondern der auch bestimmte Zusatzinformationen anzeigen kann. Diese Zusatzinformationen (d. h. Metadaten) können Informationen über den Künstler, die Abspielzeit, und weitere Informationen über die Audioaufzeichnung oder beispielsweise auch ein Bild der Schallplatten- oder der CD-Hülle sein.

Eine Verschlüsselungsvorrichtung gemäß der Erfindung des Hauptpatents ist in der Lage, Multimediadaten effizient und sicher zu verschlüsseln. Ferner implementiert die Erfindung gemäß dem Hauptpatent eine spezielle Funktionalität, welche Herausforderungs-Antwort-Verfahren genannt wird und später detailliert beschrieben ist.

Dieses Verfahren erlaubt das Erzeugen von vorverschlüsselten Audiodaten, die in einer Datenbank gespeichert sind, auf die ein Kunde sehr schnell zugreifen kann, welcher einen privaten Schlüssel verwendet, der von dem tatsächlich verwendeten Schlüssel zur Verschlüsselung der Daten abgeleitet ist, wobei sich der Kunde unter Verwendung seines privaten Schlüssels und seines Benutzerindexes den tatsächlich verwendeten Schlüssel zur Verschlüsselung selbst berechnen kann, wonach die abgerufenen Multimediadaten entschlüsselt werden können, um sie beispielsweise abzuspielen.

Damit ist es möglich, daß für viele Kunden, die das gleiche Stück abrufen, das Stück nicht jedesmal vollständig für jeden einzelnen Kunden verschlüsselt werden muß, sondern daß die Daten für alle Kunden gleich verschlüsselt werden können, wobei jedoch jeder Kunde den tatsächlich verwendeten Schlüssel unter Verwendung seines Privatschlüssels und eines von der Verschlüsselungsvorrichtung mitgeteilten Antwortschlüssels selbst berechnen kann.

Bei dem Herausforderungs-Antwort-Verfahren wird die individuelle Verschlüsselung für jeden einzelnen Benutzer also nicht durch eine vollständige Neuverschlüsselung der Multimediadaten erreicht, sondern nur durch eine vergleichsweise geringe Änderung in dem Bestimmungsdatenblock, der gemäß der vorliegenden Erfindung zu den Multimediadaten hinzugefügt wird.

Die Verschlüsselung gemäß der Erfindung des Hauptpatents erzeugt also ein Dateiformat zum Schutz von Multimediadaten, welches bei der Entschlüsselung gemäß der Erfindung des Hauptpatents verwendet wird, um beispielsweise die oben beschriebenen Funktionalitäten zu implementieren.

Der vorliegenden Erfindung liegt die Aufgabe zugrunde, Verfahren und Vorrichtungen zum Verschlüsseln und Entschlüsseln von Multimediadaten zu schaffen, welche für eine Speicherung und Übertragung in fehlerbehafteten Umgebungen und insbesondere Netzwerken geeignet sind.

Diese Aufgabe wird durch ein Verfahren zum Verschlüsseln von Multimediadaten gemäß Anspruch 1, durch ein Verfahren zum Entschlüsseln von Multimediadaten gemäß Anspruch 27, durch eine Vorrichtung zum Verschlüsseln von Multimediadaten gemäß Anspruch 33 und durch eine Vorrichtung zum Entschlüsseln von Multimediadaten gemäß Anspruch 35 gelöst.

Die Erfindung nach der vorliegenden Zusatzanmeldung ermöglicht die Übertragung und/oder Speicherung von verschlüsselten Multimediadaten auch in einer fehlerhaften Umgebung, d. h. mit fehlerbehafteten Netzwerkprotokollen. Dies wird möglich, da die Verfahren und Vorrichtungen der vorliegenden Zusatzanmeldung die verschlüsselten Daten in Pakete verpackt, die voneinander bis zu einem gewissen Grade unabhängig sind. Zu diesem Zweck umfaßt das Verfahren zum Verschlüsseln von Multimediadaten gemäß der vorliegenden Zusatzanmeldung den Schritt des Verpackens der Multimediadatei in ein Haupt-Bestimmungsdatenpaket, ein Multimediadaten-Bestimmungsdatenpaket und in ein Multimediadatenpaket, um einen paketförmig organisierten Datenstrom aus verschlüsselten Multimediadaten zu erzeugen, derart, daß das Haupt-Bestimmungsdatenpaket den Bestimmungsdaten-Verschlüsselungsindex des Bestimmungsdatenblocks aufweist, daß das Multimediadaten-Bestimmungsdatenpaket den Multimediadaten-Verschlüsselungsindex des Bestimmungsdatenblocks aufweist, und daß das Multimediadatenpaket zumindest einen Teil des Multimediadatenblocks aufweist.

Neben der Eignung der Verfahren und Vorrichtungen gemäß der vorliegenden Zusatzanmeldung für Übertragungen mit beispielsweise dem echtzeitfähigen Real Time Protocol (RTP) bietet die vorliegende Erfindung die Möglichkeit, durch dieselbe erzeugte Datenströme über drahtlose Kommunikationsmedien, wie z. B. Funknetze, zu übertragen. Ferner ermöglicht die Erfindung gemäß der Zusatzanmeldung, daß Multiplex-Bitströme, welche u. U. verschieden codierte Multimedia-Datenströme vereinen, erstellt werden können.

Ein bevorzugtes Ausführungsbeispiel der Erfindung gemäß dem Hauptpatent wird nachfolgend bezugnehmend auf die beiliegenden Zeichnungen detaillierter erläutert. Es zeigen:

Fig. 1 einen festen Teil eines Bestimmungsdatenblocks gemäß dem Hauptpatent;

Fig. 2 einen variablen Teil eines Bestimmungsdatenblocks gemäß dem Hauptpatent;

Fig. 3 eine Aufteilung von Multimediadaten in verschlüsselte Daten und unverschlüsselte Daten gemäß dem Hauptpatent;

Fig. 4 einen Hüllenblock für die verschiedenen Einträge im variablen Teil des Bestimmungsdatenblocks gemäß dem Hauptpatent; und

Fig. 5 eine Übersicht von für einzelne Funktionalitäten benötigten Einträgen in den Bestimmungsdatenblock gemäß dem Hauptpatent.

Jede Multimediaschutz-Datei (MMP-Datei; MMP = Multi Media Protection), welche im Nachfolgenden auch als MMP-Datenstrom bezeichnet wird, wird von einem speziellen MMP-Bestimmungsdatenblock begleitet. Nachfolgend wird das Format dieses Bestimmungsdatenblockes erörtert.

Der Bestimmungsdatenblock besteht aus zwei Teilen und zwar aus einem festen Teil **10**, welcher in **Fig.** 1 gezeigt ist, und aus einem variablen Teil **30**, der in **Fig.** 2 gezeigt ist. Der feste Teil **10** des Bestimmungsdatenblocks, der aus 10 und 30 besteht, enthält allgemein gesagt Minimalinformationen, wie z. B. Informationen, wie der Bestimmungsdatenblock verschlüsselt ist, wie lange derselbe ist und wo ein potentiell vorhandener nächster Bestimmungsdatenblock zu finden ist. Die Einträge in den festen Teil des Bestimmungsdatenblocks (**10**, **30**) werden nachfolgend einzeln beschrieben.

In der in **Fig.** 1 gezeigten Tabelle bezeichnet die erste Spalte den Namen des jeweiligen Eintrags, die zweite Spalte die Größe desselben, die dritte Spalte den(die) Name(n) von möglichen Untereinträgen, die vierte Spalte die jeweilige Größe des einzelnen Untereintrags, während die letzte Spalte der Tabelle in **Fig.** 1 anzeigt, ob der Eintrag, d. h. die demselben zugeordneten Untereinträge, verschlüsselt sind oder nicht.

Die erste Zeile **12** enthält einen Dateiindex, der als Untereintrag einen Identifizierer bezüglich einer speziellen MMP-Datei sowie eine Versionsnummer derselben aufweist. In Zeile **14** befindet sich ein Längenindex, welcher die Länge des Bestimmungsdatenblocks anzeigt. Dieser Eintrag dient beispielsweise zum Überspringen des Bestimmungsdatenblocks oder auch zum einfacheren parsen. In Zeile **16** be-

zeichnet ein Versatzindex den Versatz von einem Bestimmungsdatenblock zu einem nächsten Bestimmungsdatenblock, wobei derselbe nützlich ist, um z. B. im Falle von mehreren Bestimmungsdatenblöcken in einer einzigen MMP-Datei von einem Bestimmungsdatenblock zum nächsten Bestimmungsdatenblock springen zu können, ohne immer den Dateiindex auf Übereinstimmung prüfen zu müssen.

Eine Zeile **18** der Tabelle in **Fig.** 1 enthält einen Verschlüsselungsindex, welcher ein Index für eine Tabelle von Verschlüsselungs- und Entschlüsselungsalgorithmen ist, welche verwendet werden, um entscheidende Teile des Bestimmungsdatenblocks für nicht autorisierte Benutzer oder Programme unlesbar zu machen. Bei einer Implementierung der vorliegenden Erfindung können 65.535 verschiedene Verschlüsselungsalgorithmen verwendet werden, welche in einer Urheberrechtsschutzbibliothek abgelegt sind, die sowohl in der Verschlüsselungsvorrichtung als auch in der Entschlüsselungsvorrichtung gemäß der Erfindung des Hauptpatents vorhanden sein muß. Auf einen dieser 65.535 verschiedenen Verschlüsselungsalgorithmen wird über die ersten zwei Byte (d. h. den ersten Untereintrag Verfahren) zugegriffen. Der zweite Untereintrag Schlüssel liefert einen Index für eine Tabelle, in der ein Satz von Verschlüsselungsschlüsseln oder Schlüsseln für jeden Verschlüsselungsalgorithmus gespeichert sein kann. Diese Tabelle von Schlüsseln für jeden einzelnen Verschlüsselungsalgorithmus muß ebenfalls sowohl in der Verschlüsselungsvorrichtung als auch in der Entschlüsselungsvorrichtung gemäß dem Hauptpatent vorhanden sein.

Bei der Erfindung gemäß dem Hauptpatent wird also zum Ver- bzw. Entschlüsseln ein sogenanntes symmetrisches Verschlüsselungsverfahren verwendet, was bedeutet, daß sowohl die Verschlüsselungsvorrichtung als auch die Entschlüsselungsvorrichtung im Besitz sowohl der Verschlüsselungsverfahren als auch besonders der Schlüssel selbst sein müssen. Zur Ausführung der Erfindung gemäß dem Hauptpatent würde es jedoch auch genügen, lediglich den Verschlüsselungsalgorithmus in dem Verschlüsselungsindex **18** zu bestimmen. In diesem Fall könnte der Schlüssel selbst beispielsweise vorgegeben sein. Dieses Ausführungsbeispiel würde jedoch einen geringeren Schutz als das vorher beschriebene Ausführungsbeispiel mit Algorithmus und Schlüssel liefern.

Hinter dem Eintrag **18** in dem Bestimmungsdatenblock befindet sich der variable Teil **30** des Bestimmungsdatenblocks, der in **Fig.** 2 gezeigt ist und später beschrieben wird. Hinter dem variablen Teil des Bestimmungsdatenblocks befindet sich noch ein letzter Eintrag **20**, der Prüfsumme genannt wird. Diese Prüfsumme besteht z. B. aus einem sogenannten MD5-Fingerabdruck, der detaillierter in der RFC1321 beschrieben ist. Es könnte jedoch auch ein anderes Verfahren zum Berechnen der Prüfsumme verwendet werden. Zum Verständnis der vorliegenden Erfindung soll er jedoch kurz ausgeführt werden. MD5 ist ein Algorithmus, der eine beliebige Anzahl von Datenbyte in eine Zahl mit einer Länge von 128 Bit (= 16 Byte) abbildet. Die MD5-Abbildung (MD5 = Message Digest **5**) hat die Eigenschaft, daß auch die geringste Änderung in den Eingangsdaten eine völlig andere MD5-Zahl erzeugt. Daher wird MD5 benutzt, um aus Daten beliebiger Länge einen Fingerabdruck fester Größe zu erzeugen. In dem Eintrag **20** Prüfsumme befindet sich bei einem Ausführungsbeispiel der vorliegenden Erfindung beispielsweise ein MD5-Fingerabdruck des Bestimmungsdatenblocks (**10, 30**). Ein anderes Ausführungsbeispiel könnte im Eintrag Prüfsumme **20** beispielsweise sowohl den Bestimmungsdatenblock als auch eine vorbestimmte Anzahl von zu verschlüsselnden Multimediadaten aufweisen, denen der beschriebene Bestimmungsdatenblock zugeordnet ist. Dadurch definiert der Eintrag **20** eindeutig und manipuliersicher (der Eintrag **20** ist zusätzlich noch verschlüsselt) die Zuordnung eines Bestimmungsdatenblocks zu den Multimediadaten.

Alle Einträge in den Bestimmungsdatenblock, d. h. auch die Einträge des nachfolgend beschriebenen variablen Teils des Bestimmungsdatenblocks, sind in der sogenannten "Big Endian"-Bytereihenfolge. Als "Big Endian" wird eine Übertragung/Speicherung bezeichnet, bei der das höchstwertige Byte als erstes übertragen/gespeichert wird. Ein Beispiel soll dies veranschaulichen. Ein Datum ist beispielsweise vier Byte groß, d. h. sein Wert lautet $0 \times 56fe4321$. Nach der "Big Endian"-Bytereihenfolge wird 0×56 zuerst übertragen/gespeichert, woraufhin $0 \times fe$, 0×43 und 0×21 folgen. Es sei jedoch angemerkt, daß die Bytereihenfolge prinzipiell unerheblich ist.

Wie bereits angemerkt wurde, ist in **Fig.** 2 eine tabellarische Darstellung des variablen Teils **30** des Bestimmungsdatenblocks gezeigt. Die erste Spalte der Tabelle in **Fig.** 2 bezeichnet eine Identifikationsnummer (ID) der einzelnen Einträge. Die zweite Spalte enthält den Namen des Eintrags, dessen Größe in der dritten Spalte angegeben ist. Die vierte Spalte zeigt wiederum analog zu der Tabelle in **Fig.** 1 den Namen des einzelnen Untereintrags oder potentiell mehrerer Untereinträge, deren Größe wiederum in der vorletzten Spalte angegeben ist. Die letzte Spalte zeigt genauso wie in **Fig.** 1 an, ob der einzelne Eintrag verschlüsselt ist oder nicht.

Durch die Identifikationsnummer (ID) ist es möglich, jeden der in **Fig.** 2 erwähnten Einträge in den variablen Teil des Bestimmungsdatenblocks einzeln einzufügen oder wegzulassen. Die einzelnen Teile des Bestimmungsdatenblocks können somit unabhängig voneinander eingefügt oder weggelassen werden.

Der variable Teil **30** des Bestimmungsdatenblocks enthält unter anderem Informationen bezüglich der urheberrechtlichen Verschlüsselung des Audiobitstroms, d. h. der Multimediadaten. Nachfolgend werden die Einträge in den variablen Teil des Bestimmungsdatenblocks und ihre Funktionen bzw. Aufgaben im einzelnen beschrieben.

In Spalte **32** befindet sich ein Mengenindex, welcher aus zwei Untereinträgen d. h. Schritt und Menge besteht. Der erste Untereintrag Schritt gibt, wie es in **Fig.** 3 detaillierter dargestellt ist, die Gesamtmenge von Multimediadaten an, die dem speziellen Bestimmungsdatenblock zugeordnet sind. Um Multimediadaten auf einfache Weise speichern oder übertragen zu können, empfiehlt es sich, die Multimediadaten, d. h. den Bitstrom, in einzelne Datenblöcke mit überschaubarer Länge zu unterteilen, denen dann ein Bestimmungsdatenblock zugeordnet wird. Dies bedeutet, daß z. B. ein Musikstück mehrere Bestimmungsdatenblöcke aufweist, welche möglicherweise für ein einzelnes Musikstück mehrere verwendete Verschlüsselungsalgorithmen bezeichnen können.

Aufgrund der Tatsache, daß bei einem Ausführungsbeispiel der vorliegenden Erfindung die Audiodaten im MPEG Layer 3 Format vorliegen, welches bereits eine hohe Kompression der Audiodaten bewirkt, ist es im Sinne einer effizienten, zeitsparenden Ausführung der vorliegenden Erfindung ausreichend, lediglich einen bestimmten Teil eines einem Bestimmungsdatenblock zugewiesenen Datenblocks zu verschlüsseln und nicht den gesamten Datenblock zu verschlüsseln. Dies kann gemacht werden, da bei der Verwendung von hochkomprimierten Multimediaformaten schon ein sehr kleiner Teil von Störungen, d. h. Verschlüsselungen, gravierende Auswirkungen hat, da die hochkomprimierten Daten bereits eine minimale Informationsredundanz besit-

zen. Dieser Anteil der verschlüsselten Daten ist durch den Untereintrag Menge in dem Mengenindex **32** bezeichnet. **Fig.** 3 stellt also die Aufteilung eines Datenblocks in die verschlüsselten Daten und in die aus Wirtschaftlichkeitsgründen unverschlüsselt gelassenen Daten dar. Für Fachleute ist es jedoch offensichtlich, daß die vorliegende Erfindung ebenso auch eine Vollverschlüsselung vornehmen kann, bei der Schritt gleich Menge ist, während bei einer Teilverschlüsselung Schritt größer als Menge ist.

Eine Zeile **34** in Tabelle 2 bezeichnet einen Lieferantenindex, wobei der Lieferantenindex einen numerischen Wert aufweist, der auf den Inhaber der Urheberrechte der in dem Datenblock verschlüsselten Multimediadaten hinweist, der für eine Verwendung der Multimediadaten in dem Datenblock bezahlt werden muß.

In einem Eintrag **36** mit der Bezeichnung Großhändlerindex befindet sich ein numerischer Wert, der den Großhändler der in dem Datenblock vorhandenen Multimediadaten bezeichnet.

In Zeile **38** der Tabelle in **Fig.** 2 befindet sich ein Benutzerindex, welcher auf den Kunden/Benutzer hinweist, an den die in dem Datenblock vorhandenen Multimediadaten übermittelt, z. B. verkauft oder ausgeliehen, wurden.

Ein Flagindex **40** enthält zumindest drei verschiedene Flags, die als Geheim, als Registrierung und als Herausforderung bezeichnet sind. Die Flag Geheim zeigt an, daß bei der Verschlüsselung der Großhändlerindex verwendet werden soll. Wenn diese Flag gesetzt ist, wird das Verschlüsselungs/-Entschlüsselungs-Verfahren den Großhändlerindex als einen Eintrag in eine Direktzugriffstabelle benützen, um den für einen bestimmten Verschlüsselungs/Entschlüsselungs-Algorithmus erforderlichen Schlüssel zu erhalten. Dieser Eintrag ermöglicht eine Großhändler-spezifische Identifizierung von Multimediadaten, d. h. ein Benutzer/Kunde wird z. B. in der Lage sein, alle Produkte von einem spezifischen Großhändler zu beziehen.

Die Flag Registrierung zeigt an, daß sowohl der Lieferantenindex als auch der Benutzerindex bei der Verschlüsselung verwendet werden sollen. Das Verschlüsselungs/Entschlüsselungs-Verfahren wird dieses Paar (Großhändlerindex, Benutzerindex) beim Adressieren einer Direktzugriffstabelle verwenden, wodurch der Schlüssel für einen speziellen Verschlüsselungsalgorithmus erhalten werden kann. Diese Flag ermöglicht zusammen mit den jeweiligen Einträgen, daß ein Großhändler einzelne Benutzer spezifisch bedienen kann.

Die Herausforderungsflag zeigt an, daß der Kunde einen Herausforderungsindex **44** und seinen Benutzerindex verwendet hat, um eine MMP-Datei zu erhalten, wobei der Herausforderungsindex **44** und ein Antwortindexeintrag **46** in dem variablen Teil des Bestimmungsdatenblocks verschlüsselt sind. Eine detailliertere Beschreibung des Herausforderungs-Antwort-Verfahrens gemäß der Erfindung des Hauptpatents wird später durchgeführt. Selbst wenn nicht alle 32 möglichen Flags verwendet werden, muß bei einem Ausführungsbeispiel der vorliegenden Erfindung die Gesamtlänge von 4 Byte geschrieben, gesendet und gelesen werden. Alle unbenutzten Bits werden ignoriert, dieselben müssen jedoch auf Null gesetzt sein. Es ist ebenfalls möglich, alle drei Flags zu senden. In diesem Fall werden alle 3 Schlüssel verwendet, und zwar einer nach dem anderen.

Eine Zeile **42** der Tabelle von **Fig.** 2 enthält einen Freiindex. Dieser Freiindex **42** enthält zwei Untereinträge, d. h. Seriennummer und Benutzerdaten. Der Untereintrag Seriennummer enthält eine 32-Bit-lange Seriennummer, die die Multimediadaten identifiziert. Der Untereintrag Benutzerdaten, d. h. die nächsten 96 Bits des Eintrags Freiindex **42**, sind mit den ersten 12 Byte des MD5-Fingerabdrucks der ersten Daten des Multimediadatenblocks von Menge bis Schritt minus Menge gefüllt.

Der gesamte Eintrag Freiindex **42** im variablen Teil des MMP-Bestimmungsdatenblocks ist verschlüsselt, wie es in der letzten Spalte in **Fig.** 2 gezeigt ist. Ferner ist die Prüfsumme **20** des Bestimmungsdatenblocks selbst verschlüsselt, d. h. kein Unberechtigter wird in der Lage sein, eine MMP-Bestimmungsdatenblock mit einem bestimmten MD5-Fingerabdruck zu erzeugen. Der Freiindex **42** liefert damit eine eindeutige Zuordnung des Bestimmungsdatenblocks (**10**, **30**) zu den verschlüsselten oder auch unverschlüsselten Multimediadaten. Bei einer Wiedergabe, d. h. einer Entschlüsselung, wird nun überprüft, ob die aus den Multimediadaten errechnete MD5-Zahl mit der MD5-Zahl, die im Untereintrag Benutzerdaten vorhanden ist, übereinstimmt. Da bei jeder Änderung der Multimediadaten mit sehr hoher Wahrscheinlichkeit die MD5-Zahl derselben verschieden sein wird, ist anzunehmen, daß die zu schützenden Daten nicht verändert wurden, wenn die beiden MD5-Zahlen übereinstimmen.

Der Freiindex **42** wird für das bereits anfangs erwähnte Freischaltungsverfahren verwendet, welches ein Demospieler (eine Demoentschlüsselungsvorrichtung) implementieren kann. Die Untereinträge Seriennummer und Benutzerdaten in dem Freiindex **42** werden unter Verwendung der Bool'schen-Verknüpfung XOR kombiniert und mit einem Wert verglichen, der von dem Demospieler verwendet wird, d. h. auf den der Demospieler eingestellt bzw. eingerichtet ist. Wenn dieser Wert mit der Kombination von Seriennummer und Benutzerdaten übereinstimmt, wird die MMP-Datei freigeschaltet und kann uneingeschränkt (z. B. länger als etwa 20 Sekunden) gespielt werden. Falls diese Übereinstimmung nicht vorhanden ist, wird der Demospieler nicht freigeschaltet, weshalb derselbe das Abspielen, d. h. das Entschlüsseln, der Multimediadaten in der MMP-Datei abbricht. Die Freischaltung selbst dient also dazu, ein zur Wiedergabe benutztes Produkt, d. h. die Entschlüsselungsvorrichtung, zu modifizieren. Eine Entschlüsselungsvorrichtung, welche die vorliegende Erfindung ausführen kann, kann beispielsweise WinPlay **3** sein. Die Entschlüsselungsvorrichtung kann beispielsweise kostenlos als eine Demoversion bei allen Benutzern erhältlich sein. Sie wird jedoch auf eine Weitergabe von Multimediadaten mit einer Länge von beispielsweise 20 Sekunden beschränkt sein. Sobald allerdings ein MMP-Bitstrom mit gültigem Freiindex **42** erkannt wird, wird die Entschlüsselungsvorrichtung freigeschaltet. Dieselbe stellt also für die Wiedergabe einer MMP-Datei mit gültigem Freiindex **42** eine Vollversion ohne Begrenzung dar. Die Freischaltung mittels des Freiindex **42** hat also nichts mit der Bezahlung der geschützten Multimediadaten zu tun, sondern lediglich mit der Nutzung einer Demoversion der Entschlüsselungsvorrichtung. Aus technischen und politischen Gründen ist es nämlich oft einfacher, daß nicht die Verschlüsselungsvorrichtung selbst insgesamt bezahlt wird, sondern daß pro Multimediadatei eine kleine Summe für die Nutzung der Entschlüsselungsvorrichtung vom Großhändler oder Lieferanten, der den Freiindex **42** codiert hat, abgeführt wird.

In Zeile **44** und Zeile **46** der Tabelle in **Fig.** 2 befinden sich der Herausforderungsindex bzw. der Antwortindex. Der Herausforderungsindex **44** weist als Untereinträge den Codierertyp (Entschlüsselungsvorrichtungstyp), die Codiererversion, den Codiererzustand, den Großhändlerindex, den Benutzerindex und Benutzerdaten auf. Sowohl der Herausforderungsindex **44** als auch der Antwortindex **46** sind verschlüsselt.

Das Herausforderungs-Antwort-Verfahren kann verwendet werden, um eine große Datenbank von MMP-Dateien zu

erzeugen, welche Multimediadaten enthalten. Die MMP-Datenbank besteht aus MMP-Dateien, die mit einem in dem Untereintrag Schlüssel in dem Verschlüsselungsindex **18** bezeichneten Schlüssel k verschlüsselt sind. Ein Kunde wird auf diese Datenbank zugreifen, indem er zwei Hilfsschlüssel zu derselben sendet. Diese beiden Hilfsschlüssel sind der Benutzerindex u **38** und ein Benutzer-definierter Privatschlüssel p, der auch als der Herausforderungsindex **44** bezeichnet wird. Der Hilfsschlüssel u sowie der Hilfsschlüssel p sind also bei einem Kunden, d. h. bei einer speziellen Entschlüsselungsvorrichtung, vorhanden. Der Kunde sendet nun die beiden Hilfsschlüssel u und p zu einer Datenbank, die eine Vielzahl von MMP-Dateien enthält, um bestimmte Multimediadaten von derselben abzurufen. Die Datenbank, die die Multimediadateien enthält, sendet nun eine MMP-Datei zu dem Kunden zurück, welche den Antwortindex r **46** enthält. Dieser Antwortindex r wird aus der EXKLUSIV-ODER-Verknüpfung des Schlüssels k, des Benutzerindex u und des Herausforderungsindex p berechnet. Die Entschlüsselungsvorrichtung des Kunden empfängt nun die MMP-Datei von der Verschlüsselungsvorrichtung, die die MMP-Datenbank halten kann, wobei diese Datei nun den gerade berechneten Antwortindex **46** enthält. Die Entschlüsselungsvorrichtung ist nun in der Lage, den zur Entschlüsselung der Multimediadaten notwendigen Schlüssel k aus der EXKLUSIV-ODER-Verknüpfung des Antwortindex r, des Benutzerindex u und des Herausforderungsindex p ihrerseits zu berechnen. Somit liegt in der Entschlüsselungsvorrichtung des Kunden/Benutzers der Schlüssel k vor, wodurch dieselbe die dem Bestimmungsdatenblock zugeordneten Multimediadaten entschlüsseln kann.

Der Hintergrund zur Implementierung des Herausforderung-Antwort-Verfahrens liegt in einer effizienten und zeitsparenden Verschlüsselung bzw. Entschlüsselung. Eine Verschlüsselungsvorrichtung hat mit einem Schlüssel k (Verschlüsselungsindex **18**, Untereintrag Schlüssel) und mit einem Algorithmus a (Verschlüsselungsindex **18**, Untereintrag Verfahren) Multimediadaten geschützt. Diese werden zusammen mit k und a in eine MMP-Datenbank eingespeist. Möchten nun beispielsweise 1000 Kunden diese Multimediadaten beziehen, müßte ohne das Herausforderungs-Antwort-Verfahren die geschützte Kopie der Multimediadaten **1000** mal entschlüsselt und für einen speziellen Kunden wieder verschlüsselt werden. Durch das Herausforderungs-Antwort-Verfahren wird nun ein von einer speziellen Entschlüsselungsvorrichtung abhängiger Herausforderungsindex **44** zusammen mit dem daraus resultierenden Antwortindex **46** in den MMP-Datenbestimmungsblock eingetragen. Der gesamte Datenstrom der Multimediadaten muß also nicht für jeden Kunden einzeln geändert werden. Es ist also einfacher, beispielsweise 1000 mal aus einem Herausforderungsindex **44** einen Antwortindex **46** zu erzeugen und diesen in den Bestimmungsdatenblock einzutragen, als 1000 mal die gesamte MMP-Datei zu entschlüsseln und wieder kundenspezifisch zu verschlüsseln.

Eine Zeile **48** des variablen Teils des Bestimmungsdatenblocks enthält einen Auslaufindex, der das Datum kennzeichnet, zu dem die Lizenz des Benutzers, Multimediadaten zu verwenden, auslaufen wird. Derselbe ist z. B. in Sekunden gegeben, die seit Mitternacht des 1. Januar 1970 vergangen sind. Es wird darauf hingewiesen, daß der Bereich des Auslaufindex etwa bis zum Jahr 2106 ausreichend sein wird. Selbst wenn dieser Eintrag nicht verschlüsselt ist, wird es schwierig sein, denselben zu ändern, da der Auslaufindex ebenfalls die Prüfsumme **20** (den MD5-Fingerabdruck) des Bestimmungsdatenblocks verändern wird, welche zusätzlich noch verschlüsselt ist.

Eine Zeile **50** enthält einen Multimediaindex, welcher bei einem bevorzugten Ausführungsbeispiel ein ISRC-Code (ISRC = International Standard Record Code) sein kann. Dieser Multimediaindex identifiziert jedes einzelne Musikstück nach international anerkannter Norm. Der ISRC-Code identifiziert ebenfalls den Inhaber, d. h. den Lieferanten im Sinne dieser Anmeldung, des Musikstücks, der die Urheberrechte besitzt.

In einer Zeile **52** ist schließlich ein Benutzercodeindex vorgesehen, welcher verwendet wird, um ein Musikstück zu identifizieren, welches keinen ISRC-Code, d. h. keinen allgemein gültigen Multimediaindex, besitzt.

Für Fachleute ist es offensichtlich, daß der Bestimmungsdatenblock, insbesondere der variable Teil des Bestimmungsdatenblocks, beliebig erweitert werden kann, um beispielsweise weitere Metainformationen, wie z. B. Informationen über den Interpreten oder Künstler bzw. den Titel von Multimediadaten, zusammen mit der Multimediadatei zu übertragen und gegebenenfalls zu verschlüsseln. Weitere Zusatzinformationen können Informationen über das Urheberrecht, den Herausgeber eines Stücks etc. sein. Bei einem bevorzugten Ausführungsbeispiel der Erfindung gemäß dem Hauptpatent geht jedem Eintrag **32** bis **52** in dem variablen Teil **30** des Bestimmungsdatenblocks ein Hüllenblock **54** voraus, der in **Fig.** 4 gezeigt ist. Dieser Hüllenblock liefert Informationen, welcher Eintrag in den variablen Teil **30** des Bestimmungsdatenblocks demselben folgt (Eintragidentifikation), sowie Informationen über die Länge dieses speziellen Eintrags (Eintraglänge). Die Größe des Hüllendatenblocks **54** beträgt jeweils 4 Byte. Dies ist der Grund, daß die Bit-Zahl in der vorletzten Spalte der in **Fig.** 2 gezeigten Tabelle immer vier Byte kleiner als die in der dritten Spalte gezeigte Bytezahl ist.

Wie bereits angemerkt wurde, zeigen die letzte Spalte der Tabelle 1 sowie der Tabelle 2 an, ob der entsprechende Eintrag verschlüsselt ist. Die einzigen verschlüsselten Einträge in den variablen Teil des Bestimmungsdatenblocks, die verschlüsselt sind, sind der Freiindex **42**, der Herausforderungsindex **44** und der Antwortindex **46**. Alle nicht verschlüsselten Einträge sind jedoch zusätzlich durch den Eintrag Prüfsumme **20** in den festen Teil **10** des Bestimmungsdatenblocks geschützt, da die Prüfsumme zum einen verschlüsselt ist und zum anderen durch den MD5-Algorithmus bereits eine kleine Änderung der Eingabe zu einer wesentlichen Änderung des Ergebnisses desselben führen wird.

Für Fachleute ist es offensichtlich, daß z. B. auch fast alle Einträge oder mehr oder weniger als bei dem beschriebenen bevorzugten Ausführungsbeispiel verschlüsselt sein können. Eine Begrenzung der zu verschlüsselnden Daten auf die für einen ausreichenden Schutz notwendige Anzahl führt jedoch zu einer wirtschaftlichen Ausführung der Erfindung gemäß dem Hauptpatent, wie es auch im Zusammenhang mit dem Eintrag Mengenindex **32** beschrieben wurde, da es nicht notwendig ist, die gesamten Multimediadaten oder den gesamten Bestimmungsdatenblock, sondern lediglich einen Teil derselben zu verschlüsseln, um das unberechtigte Lesen der gesamten Daten unmöglich zu machen. Ferner ist es für Fachleute offensichtlich, daß es sinnlos ist, den Verschlüsselungsindex **18** selbst zu verschlüsseln, da die Entschlüsselungsvorrichtung zuerst diesen Eintrag lesen muß, um den Algorithmus und potentiell den Schlüssel für den Algorithmus zur Entschlüsselung zu erhalten.

Fig. 5 stellt zusammenfassend einige wichtige Merkmale der Erfindung gemäß dem Hauptpatent in der ersten Spalte sowie die dafür notwendigen Einträge in den variablen Teil **30** des Bestimmungsdatenblocks dar. Eine Entschlüsselungsvorrichtung gemäß der Erfindung des Hauptpatents sollte selbstverständlich auch in der Lage sein, einen unverschlüsselten Bitstrom zu lesen, wobei dann auf die in **Fig.** 5

aufgeführten Einträge insgesamt verzichtet werden kann. Soll ein verschlüsselter Bitstrom mit einem Demospieler, der die beschriebene Freischaltungsfunktion implementiert, verwendet werden, so muß der Bestimmungsdatenblock der verschlüsselten Multimediadaten zumindest den Freiindex **42** aufweisen.

Wie bereits erwähnt wurde, ist der Mengenindex **32** lediglich für eine effiziente Implementierung des Verfahrens gemäß dem Hauptpatent erforderlich. Möchte ein Großhändler alle seine Benutzer mit seinen Produkten gleichermaßen bedienen, so muß in dem Bestimmungsdatenblock der Multimediadaten der Großhändlerindex **36** besetzt sein. Optional kann auch der Freiindex **42** vorhanden sein, um lediglich bestimmten Benutzern das Abspielen von bestimmten Liedern zu erlauben.

Sollen alle Benutzer in den Genuß von Werken eines speziellen Lieferanten (d. h. des Besitzers des Urheberrechte) kommen können, können der Lieferantenindex und der Großhändlerindex besetzt sein. Optional kann auch ein Auslaufdatum **48** eingetragen sein.

Soll nur ein Benutzer auf ein spezielles Musikstück zugreifen können, so muß zusätzlich zum Lieferantenindex **34** und zum Großhändlerindex **36** der Benutzerindex **38** in den Bestimmungsdatenblock (**10, 30**) eingetragen sein.

Soll schließlich das beschriebene Herausforderungs-Antwort-Verfahren zum Einsatz kommen, was einen schnellen Zugriff auf eine große Datenbank von MMP-Multimediadateien ermöglicht, so müssen selbstverständlich die Einträge Herausforderungsindex **44** sowie Antwortindex **46** besetzt sein. Für Fachleute ist es offensichtlich, daß die Freischaltung durch den Freiindex **42** bei einem Demospieler und beispielsweise das Herausforderungs-Antwort-Verfahren beliebig kombiniert werden können.

Die Verschlüsselung bzw. Entschlüsselung gemäß dem Hauptpatent liefert also eine Möglichkeit, um Multimediadaten bereits unmittelbar nach ihrer Erzeugung vor unerlaubtem Zugriff zu schützen, wobei die gesamte Kette vom Erzeuger zum Konsumenten einschließlich der Lagerung abgedeckt ist. Die vorliegende Erfindung zeichnet sich insbesondere durch die möglichen Merkmale der Teilverschlüsselung, der Erweiterbarkeit, d. h. der variable Teil des Bestimmungsdatenblocks kann beliebige weitere Funktionen aufnehmen, der maximalen Sicherheit gegen Fälschungen (d. h. die Prüfsumme **20**) und der Verschlüsselung bestimmter Einträge in dem Bestimmungsdatenblock auf. Damit sind sowohl ein Schutz gegen eine unerlaubte Verwendung von Multimediadaten als auch durch Verwendung des Herausforderungs-Antwort-Gedankens eine effiziente Implementierung der Erfindung gemäß dem Hauptpatent erreicht.

Im nachfolgenden wird die Erfindung gemäß der vorliegenden Zusatzpatentanmeldung beschrieben. Durch das Verfahren zum Verschlüsseln von Multimediadaten gemäß der vorliegenden Erfindung werden die verschlüsselten Multimediadaten in verschiedene Pakete gepackt. Zunächst werden ein Haupt-Bestimmungsdatenpaket (MMP Header Packet oder MHP), ein Multimediadaten-Bestimmungsdatenpaket (MMP Payload Header Packet oder MPHP), ein Multimediadatenpaket (MMP Payload Data Packet oder MPDP) und vorzugsweise ein Übertragungsendepaket (MMP End of Transfer Packet oder MEOT) definiert. Das Haupt-Bestimmungsdatenpaket (MHP) umfaßt Grundinformationen eines durch das Verfahren zum Verschlüsseln von Multimediadaten gemäß der vorliegenden Erfindung erzeugten Datenstroms. Ein derartiger Datenstrom enthält zumindest ein Multimediadaten-Bestimmungsdatenpaket (MPHP), wobei jedes Multimediadaten-Bestimmungsdatenpaket wiederum einem Multimediadatenpaket (MPDP) zugeordnet ist. Das Übertragungsendepaket dient zum Anzeigen des Endes eines durch das Verfahren zum Verschlüsseln von Multimediadaten erzeugten Datenstroms. Ein derartiger Datenstrom kann also auch mehrere "elementare Nutzdatenströme" enthalten, welche beispielsweise codierte/uncodierte und/oder verschlüsselte Musikstücke, Videosequenzen, Sprachwerke und dergleichen sein können.

Das Haupt-Bestimmungsdatenpaket und das Multimediadaten-Bestimmungsdatenpaket enthalten Informationen des Bestimmungsdatenblocks (**10, 30**). Insbesondere umfaßt das Haupt-Bestimmungsdatenpaket den Bestimmungsdaten-Verschlüsselungsindex des Bestimmungsdatenblocks. Das Multimediadaten-Bestimmungsdatenpaket umfaßt dagegen den Multimediadaten-Verschlüsselungsindex des Bestimmungsdatenblocks. Das Multimediadatenpaket wiederum umfaßt zumindest einen Teil des Multimediadatenblocks, der dem Bestimmungsdatenblock zugeordnet ist. Der Freiindex kann im Haupt-Bestimmungsdatenpaket sein, wenn eine Freischaltung des gesamten Datenstroms angestrebt wird. Wird jedoch eine Freischaltung erwünscht, die sich nur auf einzelne Stücke bezieht, so wird der Freiindex in das Multimediadaten-Bestimmungsdatenpaket gepackt, das dem entsprechenden Stück zugeordnet ist. Eine Kombination der genannten Möglichkeiten eröffnet sich ebenfalls, wenn in mindestens zwei Bestimmungsdatenpaketen ein Freiindex vorgesehen wird.

Im nachfolgenden wird im einzelnen der weitere Inhalt der jeweiligen Pakete dargelegt. Alle Pakete, die sich in einem Datenstrom befinden, der durch das Verfahren gemäß der vorliegenden Erfindung erzeugt worden ist, beginnen vorzugsweise mit einem festen Satz an Daten. Unter diesen Daten befindet sich zunächst eine Versionsnummer, für die eine Länge von 4 Byte vorgesehen ist, um zu kennzeichnen, mit welcher MMP-Algorithmusversion das entsprechende Paket erzeugt worden ist. Dieser Eintrag verhindert eine Vermischung von Paketen, die von unterschiedlichen Algorithmusversionen erzeugt worden sind. Der feste Satz an Daten umfaßt ferner eine Pakettyp-Kennung, für die eine Länge von 4 Bit vorgesehen ist. Die Pakettyp-Kennung gibt an, um welchen Pakettyp (MHP, MPHP, MPDP oder MEOT) es sich bei dem vorliegenden Paket handelt. Der feste Satz an Daten umfaßt ferner eine Paket-Seriennummer mit einer Länge von 2 Byte, die innerhalb eines durch das Verfahren zum Verschlüsseln gemäß der vorliegenden Erfindung erzeugten Datenstroms eindeutig generiert werden soll. Diese Nummer sollte ferner (pseudo-) zufällig erzeugt werden.

Der feste Satz an Daten umfaßt vorzugsweise ferner eine Datenstrom-Seriennummer mit einer Länge von 2 Byte, wodurch alle Pakete eines speziellen Datenstroms einander zugeordnet werden. Diese Datenstrom-Seriennummer sollte ebenfalls (pseudo-) zufällig erzeugt werden. Der feste Satz an Daten umfaßt ebenfalls die Länge des entsprechenden Pakets in Byte, wobei für die Längenangabe selbst 2 Byte vorgesehen sind. Der feste Satz an Daten kann schließlich einen Verfallsindex umfassen, nach dem das Paket seine "Gültigkeit" verliert. Diese Angabe sollte in verstrichenen Sekunden seit Mitternacht des 1. Januars 1970 erfolgen. Die Länge des Verfallsdatums beträgt 4 Byte. Zu guter Letzt umfaßt der feste Satz an Daten einen verschlüsselten Fingerabdruck des entsprechenden Pakets mit einer Länge von 16 Byte, welcher z. B. mit Hilfe von MD5 berechnet und vorzugsweise mittels eines symmetrischen Verschlüsselungsverfahrens geschützt wird. Dieses Paket gemäß der vorliegenden Erfindung ist also durch einen MD5-Fingerabdruck erfaßt und geschützt, da eben dieser Fingerabdruck selbst verschlüsselt ist. Eine unerlaubte Modifikation eines Paketeintrags wird zu einem anderen Fingerabdruck führen, der

bei seiner Entschlüsselung keine sinnvollen Daten mehr ergeben wird. Die Herstellung des Fingerabdrucks und die Verschlüsselung desselben stellt somit einen wirksamen Schutz für jedes Paket an sich dar.

Nachdem die Informationen beschrieben worden sind, die vorzugsweise in jedem Pakettyp enthalten sind, werden im nachfolgenden die pakettypspezifischen Informationen dargelegt.

Das Haupt-Bestimmungsdaten-Paket umfaßt den Bestimmungsdaten-Verschlüsselungsindex des Bestimmungsdatenblocks. Der Bestimmungsdaten-Verschlüsselungsindex weist auf einen zum Verschlüsseln zumindest eines Abschnitts des Bestimmungsdatenblocks zu verwendenden Bestimmungsdaten-Verschlüsselungsalgorithmus hin. Insbesondere ist hier eine Tabelle für die gültigen Verschlüsselungsalgorithmen zu erstellen, welche z. B. zumindest DES (Data Encryption Standard) und "Blowfish" oder auch andere Methoden enthält. Das Haupt-Bestimmungsdaten-Paket (MHP) umfaßt ferner vorzugsweise die Größe des Haupt-Bestimmungsdatenpakets sowie die Menge der verschlüsselten Daten des Haupt-Bestimmungsdatenpakets. Es ist somit möglich, zu bestimmen, wie viele Daten verschlüsselt werden, und wie viele unverschlüsselt bleiben.

Vorzugsweise wird ferner eine Kennummer des "Media Distributors" oder "Händlers" eingetragen, welche eine Länge von 4 Byte hat. Ein "Media Distributor" ist nach offizieller ISO/MPEG-Terminologie eine Unternehmung oder eine Person, die Multimediadaten für die Öffentlichkeit nutzbar macht, also zum Kauf anbietet, verschenkt, vermietet, usw. Das Haupt-Bestimmungsdatenpaket umfaßt ferner die Anzahl der Kunden-Kennummern oder Benutzerindizes mit einer Länge von 1 Byte. Außerdem befindet sich im Haupt-Bestimmungsdatenpaket eine Liste der Kunden-Kennummern oder Benutzerindizes, welche den verschlüsselten Datenstrom empfangen sollen. Für jede Kunden-Kennummer sind 4 Byte vorgesehen.

Wie es bereits erwähnt wurde, können einem Haupt-Bestimmungsdatenpaket mehrere "elementare Nutzdatenströme" untergeordnet werden. Es ist daher möglich, daß ein Kunde über einen einzigen MMP-Datenstrom mehrere verschiedene Musikstücke, d. h. verschiedene elementare Nutzdatenströme, erhält. Für die Anzahl der verschiedenen elementaren Nutzdatenströme ist ein Byte vorgesehen. Jeder elementare Nutzdatenstrom enthält ferner eine Kennummer (1 Byte für jeden elementaren Nutzdatenstrom). Diese Kennummer muß innerhalb eines MMP-Datenstroms eindeutig sein. Sind demnach einem Haupt-Bestimmungsdatenpaket beispielsweise 5 elementare Nutzdatenströme untergeordnet, so wird das Haupt-Bestimmungsdatenpaket 5 verschiedene Kennummern umfassen. Ein Haupt-Bestimmungsdatenpaket umfaßt ferner vorzugsweise Übertragungsmedium-spezifische Informationen. Für eine Internet-Übertragung können diese Informationen vom MIME-Typ (MIME = Multipurpose Internet Mail Extensions) sein. Diese übertragungsspezifischen Informationen sind beim MIME-Typ ein bis zu 255 Byte langer ASCII-Text für jeden elementaren Nutzdatenstrom, z. B. "audio/x-mpeg" für den Codierstandard MPEG Layer-3. Die Länge der Angabe des MIME-Typs für den Nutzdatenstrom (1 Byte für jeden elementaren Nutzdatenstrom) bildet ferner vorzugsweise ebenfalls einen Teil des Haupt-Bestimmungsdatenpakets.

Jedem elementaren Nutzdatenstrom ist ferner mindestens ein Multimediadaten-Bestimmungsdatenpaket zugeordnet. Dieses Multimediadaten-Bestimmungsdatenpaket umfaßt die Kennummer des entsprechenden elementaren Nutzdatenstroms (Länge = 1 Byte). Durch diese Kennummer ist das Multimediadaten-Bestimmungsdatenpaket dem Multimediadaten-Paket zugeordnet, das ja die zumindest teilweise verschlüsselten Nutzdaten trägt. Jedes Multimediadaten-Bestimmungsdatenpaket umfaßt ferner eine Sequenznummer mit einer Länge von 2 Byte, um die Reihenfolge des entsprechenden elementaren Nutzdatenstroms in dem verschlüsselten Datenstrom anzuzeigen. Außerdem umfaßt ein Multimediadaten-Bestimmungsdatenpaket Urheberinformationen bezüglich des elementaren Nutzdatenstroms, welcher beispielsweise ein Musikstück, eine Videosequenz oder ähnliches sein kann. Informationen, die typisch für den Nutzdatenstrom sind, z. B. Angabe über Autoren, Komponisten, Angaben über die Inhaber der Rechte an dem elementaren Strom, Angaben über das Stück selbst, z. B. den ISRC, usw., können ferner in das Multimediadaten-Bestimmungsdatenpaket für den entsprechenden elementaren Nutzdatenstrom geschrieben werden.

Das Multimediadatenpaket, das ja normalerweise hauptsächlich die eigentlichen Nutzdaten enthält, umfaßt neben den Informationen, die für alle Pakettypen gegeben sind, lediglich die Kennummer des elementaren Nutzdatenstroms mit der Länge von 1 Byte. Durch diese Kennummer oder Kennung werden, wie es bereits erwähnt wurde, Verknüpfungen zwischen einem elementaren Nutzdatenstrom, d. h. dem Multimediadatenpaket, das den verschlüsselten elementaren Nutzdatenstrom enthält, und dem jeweiligen Multimediadaten-Bestimmungsdatenpaket hergestellt. An dieser Stelle sei noch einmal darauf hingewiesen, daß dagegen die Zuordnung zwischen dem Haupt-Bestimmungsdatenpaket und dem zumindest einen Multimediadaten-Bestimmungsdatenpaket in einem Datenstrom hergestellt wird, indem die Kennummer des elementaren Nutzdatenstroms auch in das Haupt-Bestimmungsdatenpaket geschrieben, d. h. gepackt, wird.

Die Übertragungsendepakete (MEOT) können entweder leer sein oder eine Nachricht beinhalten, die den Kunden oder Empfänger eines verschlüsselten Datenstroms vom Ende des Datenstroms unterrichtet. Im letzteren Fall müssen Länge und Daten dieser Information codiert werden.

Jedes durch das erfindungsgemäße Verfahren zum Verschlüsseln erzeugte Paket wird mit einem Schlüssel verschlüsselt, der aus dem Sitzungsschlüssel und der laufenden Nummer des Pakets berechnet wird, wie z. B. mittels einer Exklusiv-Oder-Verknüpfung. Auf den Schlüssel, der zur Verschlüsselung eines Pakets verwendet wird, wird durch den Verschlüsselungsindex verwiesen. Der bzw. die Schlüssel wird bzw. werden der MMP-Verschlüsselungsvorrichtung bzw. der MMP-Entschlüsselungsvorrichtung über MMP-Registration-Strings (weiter hinten detailliert beschrieben) übergeben. Beim Haupt-Bestimmungsdatenpaket kann dies der Bestimmungsdaten-Verschlüsselungsindex des Bestimmungsdatenblocks sein. Beim Multimediadaten-Bestimmungsdatenblock kann dieser Schlüssel durch den Multimediadaten-Verschlüsselungsindex des Bestimmungsdatenblocks bezeichnet sein. Dann wäre das Multimediadaten-Bestimmungsdatenpaket mit dem gleichen Schlüssel wie das Multimediadatenpaket selbst verschlüsselt. Für Fachleute ist es offensichtlich, daß für den Multimediadatenblock selbst ein weiterer Schlüssel gewählt werden kann, der in dem Multimediadaten-Bestimmungsdatenpaket angegeben ist, welches jedoch durch einen abweichenden Schlüssel verschlüsselt ist. Für Fachleute ist es ferner offensichtlich, daß für die Verschlüsselung aller Pakete derselbe Schlüssel und/oder derselbe Verschlüsselungsalgorithmus gewählt werden kann, und daß insbesondere der Bestimmungsdaten-Verschlüsselungsindex und der Multimediadaten-Verschlüsselungsindex bis auf die Paketnummer selbst übereinstimmen können. Solche Vereinfachungen könnten jedoch dazu führen, daß MMP-Pakete gegenüber einer unerwünschten bzw. unerlaubten Modifikation anfälli-

ger werden.

Wie es bereits erwähnt wurde, kommen als Verschlüsselungsverfahren der Data Encryption Standard (DES mit einer Schlüssellänge von 56 Bit) oder der Blowfish-Algorithmus (mit einer Schlüssellänge von 64 Bit) in Frage. Bei einem Ausführungsbeispiel der Erfindung gemäß dem Hauptpatent wurde der Bestimmungsdatenblock mit sog. "Standardschlüsseln" vor illegalem Zugriff geschützt, die in jedem MMP-fähigen Programm vorliegen müssen. Gemäß einem bevorzugten Ausführungsbeispiel der vorliegenden Erfindung der Zusatzpatentanmeldung werden dagegen sämtliche Daten (Nutzdaten und Bestimmungsdaten) mit nachfolgend beschriebenen Großhändler- und/oder Benutzerindizes bzw. -Schlüsseln verschlüsselt. Das Verfahren zum Verschlüsseln gemäß der vorliegenden Erfindung ermöglicht eine "Personalisierung" von Multimediadaten. Um diese personalisierten Multimediadaten abspielen zu können, muß eine entsprechende Entschlüsselungsvorrichtung ebenfalls personalisiert werden. Dies geschieht über sog. "MMP Registration Strings", welche z. B. auf dem Lieferantenindex, dem Großhändlerindex und/oder dem Benutzerindex basieren können. Damit Großhändler Multimedia-Datenströme erzeugen können, besitzen dieselben solche MMP-Registration-Strings, die den Großhändlerindex und den entsprechenden Schlüssel beinhalten. Um nun einem Kunden zu erlauben, eine für ihn personalisierte MMP-Multimediadatei abspielen zu können bzw. einen verschlüsselten Datenstrom empfangen und abspielen zu können, soll der entsprechende MMP Registration String sowohl die Kennummer und den Schlüssel des Großhändlers bzw. Lieferanten als auch die Kundennummer und den Kundenschlüssel des Kunden enthalten. Wird ein MMP-Registration-String ohne Kundeninformationen erstellt, so können (Radio-ähnlich) MMP-Dateien an alle Kunden dieses Großhändlers bzw. Lieferanten verteilt werden, während im Falle von kundenspezifischen Informationen in dem MMP-Registration-String der Verkauf nur an einen speziellen Kunden möglich ist.

Der Aufbau eines MMP-Registration-Strings wird nachfolgend dargestellt. Derselbe besteht vorzugsweise aus 5 Teilen, und zwar aus DUxCV. V hat eine Länge von 1 Byte und gibt die Version des MMP-Registration-Strings an. D umfaßt ebenfalls eine Länge von 1 Byte und gibt die Länge des Mediadistributor-Schlüssels bzw. des Großhändlerindex an. U hat ebenfalls eine Länge von 1 Byte und gibt die Länge des Kunden-Schlüssels, d. h. des Benutzerindex, an. x hat schließlich eine variable Länge und beinhaltet zum einen eine Kennummer des ausgebenden Mediengroßhändlers, welche ebenfalls der Großhändlerindex oder ein anderer Index sein kann. Die Länge dieser Kennummer beträgt vorzugsweise 32 Bit. x umfaßt ferner den Zugangsschlüssel des Mediengroßhändlers, wobei die Länge dieses Zugangsschlüssels durch den Teil D angegeben wird. Außerdem umfaßt x die Kundenkennummer mit einer Länge von 32 Bit, welche auch als Benutzerindex bezeichnet wird. x umfaßt ferner einen Zugangsschlüssel des Kunden, wobei die Länge des Zugangsschlüssels durch den Teil C gegeben ist. Falls U den Wert Null enthält, beinhaltet x weder eine Kundenkennnummer noch einen Kunden-Zugangsschlüssel. C schließlich beinhaltet einen MD5-Fingerabdruck von D, U, x und V und besitzt eine variable Länge.

Da die einzelnen Elemente des MMP-Registration-Strings aus nicht-druckbaren Zeichen bestehen können, wird vorzugsweise ein base64-Algorithmus verwendet, um den MMP-Registration-String handhabbar zu machen. Der base64-Algorithmus transformiert jeweils 3 Byte in 4 druckbare Zeichen. Eine Bitkette aus n Byte (n muß durch 3 teilbar sein) wird daher um den Faktor 4/3 verlängert. Mit Hilfe des base64-Algorithmus kann somit jede beliebige Bitkombination, deren Länge durch 24 teilbar ist, mit Hilfe des ASCII-Zeichensatzes übertragen und gespeichert werden.

Die MMP-Registration-Strings werden vorzugsweise durch ein asymmetrisches Verschlüsselungsverfahren, z. B. RSA (RSA = Rivest-Shamir-Adleman), gegen unberechtigten Zugriff geschützt. Ein Endkunde kann daher nur die MMP-Registration-Strings lesen, aber keine eigenen derartigen Verschlüsselungsindizes erzeugen. Da asymmetrische Verschlüsselungsverfahren nur bei langen Schlüsseln ausreichend sicher sind (ab einer Länge von 1024 Bit), wird der MMP-Registration-String durch Pseudozufallszahlen auf die benötigte Länge gebracht.

Aufgrund der Tatsache, daß die Länge der MMP-Registration-Strings (rund 180 Zeichen), welche in dieser Anmeldung ebenfalls als Verschlüsselungsindizes bezeichnet werden, recht unhandlich geworden sind, können diese Verschlüsselungsindizes kaum mehr von einem Benutzer manuell eingetippt werden. Sie müssen daher über ein Installationsprogramm den MMP-Entschlüsselungsvorrichtungen zugeführt werden. Daher spielt es keine Rolle, noch einen weiteren Teil an die Verschlüsselungsindizes anzuhängen. Der "natürliche" Name des Besitzers des Verschlüsselungsindex eignet sich dafür besonders. Dadurch, daß der Name des Besitzers in dem Verschlüsselungsindex oder MMP-Registration-String auftritt, wird die psychologische Hemmschwelle angehoben, den eigenen MMP-Registration-String weiterzugeben. Vorzugsweise wird dieser zusätzliche Teil weder verschlüsselt noch mittels des base64-Algorithmus codiert. Derselbe sollte jedoch in dem Fingerabdruck C einbezogen werden.

Wie es bereits an mehreren Stellen erwähnt wurde, ermöglicht die hierarchische Struktur des Datenstroms, der erfindungsgemäß erzeugt wird, mehrere Multimediadaten-Bestimmungsdatenpakete in einem einzigen Datenstrom zu verwenden, wobei jedes Multimediadaten-Bestimmungsdatenpaket eine eigene eindeutige Kennung hat, welche u. a. auch das verwendete Codierungsverfahren angibt. Da somit jedes Multimediadatenpaket oder Nutzdatenpaket die Kennnummer eines Multimediadaten-Bestimmungsdatenpakets mit sich führt, können also mehrere Bitströme innerhalb eines Datenstroms, der gemäß der vorliegenden Erfindung erzeugt wird, übertragen und wieder entschlüsselt werden.

Ein Vorteil des Datenstroms, der gemäß der vorliegenden Erfindung erzeugt wird, besteht ferner darin, daß eine sehr hohe Sicherheit gegenüber einer unerlaubten Verschlüsselung vorhanden ist. Dies ist der Fall, da die Verschlüsselungsindizes oder MMP-Registration-Strings "von außen" eingegeben werden müssen und zugleich über den MD5-Fingerabdruck von den zu entschlüsselnden Daten abhängen. Diese einzugebenden Schlüssel werden ferner vorzugsweise mittels bekannter asymmetrischer Verschlüsselungsverfahren vor illegalen Veränderungen geschützt, wie es bereits dargelegt wurde. Datenströme aus den gemäß der vorliegenden Erfindung erzeugten Paketen können somit zum einen außerordentlich sicher gegenüber einem unerlaubten Zugriff gestaltet werden und zum anderen aufgrund der hierarchischen Paketstruktur in einer fehlerhaften Umgebung übertragen bzw. gespeichert werden.

Patentansprüche

1. Verfahren zum Verschlüsseln von Multimediadaten, um eine verschlüsselte Multimediadatei zu erhalten, die einen Bestimmungsdatenblock (**10**, **30**) und einen Multimediadatenblock aufweist, mit folgenden Schritten:

Eintragen eines Bestimmungsdaten-Verschlüsselungsindex (**18**) in den Bestimmungsdatenblock (**10**, **30**),

welcher auf einen zum Verschlüsseln eines Abschnitts des Bestimmungsdatenblocks (**10, 30**) zu verwendenden Bestimmungsdaten-Verschlüsselungsalgorithmus hinweist;

Eintragen eines Multimediadaten-Verschlüsselungsindex (**34, 36, 38, 44, 46**) in den Bestimmungsdatenblock (**10, 30**), welcher auf einen zum Verschlüsseln zumindest eines Teils des Multimediadatenblocks zu verwendenden Multimediadaten-Verschlüsselungsalgorithmus hinweist;

Eintragen eines Freiindex (**42**) in den Bestimmungsdatenblock (**10, 30**), wobei der Freiindex (**42**) eine bestimmte Entschlüsselungsvorrichtung identifiziert, mit der ein Entschlüsseln der verschlüsselten Multimediadaten über eine vorbestimmte Zeitdauer hinaus möglich ist;

Auswählen des Bestimmungsdaten-Verschlüsselungsalgorithmus aus einer Mehrzahl von Verschlüsselungsalgorithmen aufgrund des Bestimmungsdaten-Verschlüsselungsindex (**18**);

Auswählen des Multimediadaten-Verschlüsselungsalgorithmus aus einer Mehrzahl von Verschlüsselungsalgorithmen aufgrund des Multimediadaten-Verschlüsselungsindex (**34, 36, 38, 44, 46**);

Verschlüsseln des Abschnitts des Bestimmungsdatenblocks (**10, 30**) mit dem Bestimmungsdaten-Verschlüsselungsalgorithmus, wobei der Abschnitt des Bestimmungsdatenblocks (**10, 30**) den Bestimmungsdaten-Verschlüsselungsindex nicht aufweist; und

zumindest teilweises Verschlüsseln des Multimediadatenblocks mit dem Multimediadaten-Verschlüsselungsalgorithmus, nach dem Hauptpatent 19625635.6-31,

gekennzeichnet durch folgenden Schritt:

Verpacken der Multimediadatei in ein Haupt-Bestimmungsdatenpaket, in ein Multimediadaten-Bestimmungsdatenpaket und in ein Multimediadatenpaket, um einen Datenstrom aus verschlüsselten Multimediadaten zu erzeugen, derart, daß

- das Haupt-Bestimmungsdatenpaket den Bestimmungsdaten-Verschlüsselungsindex des Bestimmungsdatenblocks (**10, 30**) aufweist,
- das Multimediadaten-Bestimmungsdatenpaket den Multimedia-Verschlüsselungsindex des Bestimmungsdatenblocks (**10, 30**) aufweist; und
- das Multimediadatenpaket zumindest einen Teil des Multimediadatenblocks aufweist.

2. Verfahren gemäß Anspruch 1, das ferner folgenden Schritt aufweist:

Erzeugen eines Übertragungsendepakets, das einem Empfänger das Ende eines verschlüsselten Multimediadatei signalisiert.

3. Verfahren nach Anspruch 1 oder 2, das ferner folgenden Schritt aufweist:

Eintragen einer Kennung in das Haupt-Bestimmungsdatenpaket, das Multimediadaten-Bestimmungsdatenpaket und das Multimediadatenpaket, um das Multimediadatenpaket dem Multimedia-Bestimmungsdatenpaket einerseits und das Multimediadaten-Bestimmungsdatenpaket dem Haupt-Bestimmungsdatenpaket andererseits eindeutig zuzuordnen.

4. Verfahren nach einem der vorhergehenden Ansprüche, bei dem der Datenstrom mehrere elementare Nutzdatenströme aufweist, wobei je ein Multimediadatenpaket je einem elementaren Nutzdatenstrom und je einem Multimediadaten-Bestimmungsdatenpaket zugeordnet ist, das ferner folgende Schritte aufweist:

Eintragen einer eindeutigen Kennung in jedes Multimediadatenpaket und in jedes Multimediadaten-Bestimmungsdatenpaket, um jedem elementaren Nutzdatenstrom ein eigenes Multimediadaten-Bestimmungsdatenpaket zuzuordnen; und

Eintragen aller Kennungen der Multimediadaten-Bestimmungsdatenpakete, die einem Haupt-Bestimmungsdatenpaket zugeordnet sind, in das Haupt-Bestimmungsdatenpaket.

5. Verfahren nach einem der vorhergehenden Ansprüche, das ferner folgenden Schritt aufweist:

Eintragen von Übertragungsmedium-spezifischen Informationen in das Haupt-Bestimmungsdatenpaket.

6. Verfahren nach Anspruch 4 oder 5, das ferner folgenden Schritt aufweist:

Eintragen einer Sequenznummer in jedes Multimediadaten-Bestimmungsdatenpaket, um die Reihenfolge des entsprechenden elementaren Nutzdatenstroms in dem verschlüsselten Datenstrom anzuzeigen.

7. Verfahren nach einem der vorhergehenden Ansprüche, das ferner folgenden Schritt aufweist:

Eintragen einer Versionsnummer in jedes Paket, um Pakete derselben MMP-Version zu identifizieren.

8. Verfahren nach einem der vorhergehenden Ansprüche, das ferner folgenden Schritt aufweist:

Eintragen einer Pakettyp-Kennung in jedes Paket, um anzuzeigen, welchen Typs das vorliegende Paket ist.

9. Verfahren nach einem der vorhergehenden Ansprüche, das ferner folgenden Schritt aufweist:

Eintragen einer Paketseriennummer, die für jeden Pakettyp eines elementaren Nutzdatenstroms eindeutig ist.

10. Verfahren nach einem der vorhergehenden Ansprüche, das ferner folgenden Schritt aufweist:

Eintragen eines Paketlängenindex in jedes Paket, der die Länge des entsprechenden Pakets angibt.

11. Verfahren nach einem der vorhergehenden Ansprüche, das ferner folgende Schritte aufweist:

Eintragen eines Verfallsindex in jedes Paket, der die Gültigkeitsdauer des entsprechenden Pakets angibt.

12. Verfahren nach einem der vorhergehenden Ansprüche, bei dem der Bestimmungsdaten-Verschlüsselungsindex und/oder der Multimediadaten-Verschlüsselungsindex Angaben über die Quelle der Multimediadaten und eine jedem Paket zugeordnete Paketnummer aufweisen, um eine Entschlüsselung des Multimediadatenstroms durch alle Kunden der Quelle der Multimediadaten zu erlauben.

13. Verfahren nach Anspruch 12, bei dem der Bestimmungsdaten-Verschlüsselungsindex und der Multimediadaten-Verschlüsselungsindex außerdem Angaben über den einzelnen Kunden aufweisen, um eine Entschlüsselung der Multimediadaten lediglich durch einen speziellen Kunden zu erlauben.

14. Verfahren nach einem beliebigen der Ansprüche 1–13, das ferner folgende Schritte aufweist:

Eintragen eines Mengenindex (**32**) in den Bestimmungsdatenblock (**10, 30**), der einen Anteil der zu verschlüsselnden Multimediadaten von der Gesamtheit der Multimediadaten in dem Multimediadatenblock anzeigt, wodurch lediglich der durch den Mengenindex (**32**) bezeichnete Anteil der Multimediadaten mittels des Multimediadaten-Verschlüsselungsalgorithmus verschlüsselt wird; und

Verpacken des Mengenindex in das Multimediadaten-Bestimmungsdatenpaket.

15. Verfahren gemäß einem beliebigen der vorhergehenden Ansprüche, das ferner folgende Schritte aufweist:

Eintragen eines Lieferantenindex (**34**) in den Bestim-

mungsdatenblock (**10, 30**), der den Lieferanten anzeigt, der die Urherberrechte für die Multimediadaten besitzt; und

Verpacken des Lieferantenindex in das Haupt-Bestimmungsdatenpaket.

16. Verfahren gemäß einem beliebigen der vorhergehenden Ansprüche, das ferner folgende Schritte aufweist:

Eintragen eines Großhändlerindex (**36**) in den Bestimmungsdatenblock (**10, 30**), der den Großhändler anzeigt, der die Multimediadaten anbietet; und

Verpacken des Großhändlerindex in das Haupt-Bestimmungsdatenpaket.

17. Verfahren gemäß einem beliebigen der vorhergehenden Ansprüche, das ferner folgende Schritte aufweist:

Eintragen eines Benutzerindex (**38**) in den Bestimmungsdatenblock (**10, 30**), der den Benutzer anzeigt, zu dem die Multimediadaten geliefert werden sollen; und

Verpacken des Benutzerindex in das Haupt-Bestimmungsdatenpaket.

18. Verfahren gemäß Anspruch 6, das ferner folgende Schritte aufweist:

Eintragen eines Herausforderungsindex (**44**) und eines Antwortindex (**46**) in den Bestimmungsdatenblock (**10, 30**), wobei der Herausforderungsindex (**44**) und der Benutzerindex (**38**) zum Benutzer-selektiven Abrufen von Multimediadaten verwendet werden und zusammen mit dem Antwortindex (**46**) zum Entschlüsseln mittels eines zu verwendenden Entschlüsselungsalgorithmus verwendet werden, wobei aus dem Antwortindex (**46**) in Verbindung mit dem Benutzerindex (**38**) und dem Herausforderungsindex (**44**) ein Schlüssel (k) für den Verschlüsselungsalgorithmus zum Entschlüsseln bestimmt wird; und

Verpacken des Herausforderungsindex und des Antwortindex in das Haupt-Bestimmungsdatenpaket.

19. Verfahren gemäß Anspruch 18, das ferner folgende Schritte aufweist:

Eintragen eines Flagindex (**40**) in den Bestimmungsdatenblock (**10, 30**), der anzeigt, ob bei der Verschlüsselung der Großhändlerindex (**36**), der Großhändlerindex (**36**)

und der Benutzerindex (**38**) oder der Herausforderungsindex (**44**) und der Antwortindex (**46**) verwendet werden sollen; und

Verpacken des Flagindex in das Haupt-Bestimmungsdatenpaket.

20. Verfahren gemäß einem beliebigen der vorhergehenden Ansprüche, das ferner folgende Schritte aufweist:

Eintragen eines Auslaufindex (**48**) in den Bestimmungsdatenblock (**10, 30**), der anzeigt, wann eine Lizenz eines Benutzers zum Abrufen der Multimediadaten ausläuft; und

Verpacken des Auslaufindex in das Haupt-Bestimmungsdatenpaket.

21. Verfahren gemäß einem beliebigen der vorhergehenden Ansprüche, das ferner folgende Schritte aufweist:

Eintragen eines Multimediaindex (**50**) in den Bestimmungsdatenblock (**10, 30**), der einzelne Musikstücke nach internationalem Standard identifiziert; und

Verpacken des Multimediaindex in das Multimediadaten-Bestimmungsdatenpaket.

22. Verfahren gemäß Anspruch 21, das ferner folgende Schritte aufweist:

Eintragen eines Benutzercodeindex (**52**) in den Bestimmungsdatenblock (**10, 30**), der Musikstücke identifiziert, die keinen Multimediaindex (**50**) aufweisen; und

Verpacken des Benutzercodeindex in das Multimediadaten-Bestimmungsdatenpaket.

23. Verfahren gemäß einem beliebigen der vorhergehenden Ansprüche, das ferner folgenden Schritt aufweist:

Erzeugen und Eintragen einer jeweiligen Prüfsumme in das Haupt-Bestimmungsdatenpaket, das Multimediadaten-Bestimmungsdatenpaket und das Multimediadatenpaket.

24. Verfahren gemäß Anspruch 23, das ferner folgenden Schritt aufweist:

Verschlüsseln der Prüfsumme (**20**), des Freiindex (**42**), des Herausforderungsindex (**44**) und des Antwortindex (**46**); und

Eintragen der verschlüsselten Indizes in den Bestimmungsdatenblock (**10, 30**).

25. Verfahren gemäß Anspruch 23 oder 24,

bei dem der Dateiindex (**12**), der Längenindex (**14**), der Versatzindex (**16**), der Verschlüsselungsindex (**18**) und die Prüfsumme (**20**) in einem festen Teil des Bestimmungsdatenblocks vorhanden sind, während sich der Mengenindex (**32**), der Lieferantenindex (**34**), der Großhändlerindex (**36**), der Benutzerindex (**38**), der Flagindex (**40**), der Freiindex (**42**), der Herausforderungsindex (**44**), der Antwortindex (**46**), der Auslaufindex (**48**), der Multimediaindex (**50**) und der Benutzercodeindex (**52**) in einem variablen Teil (**30**) des Bestimmungsdatenblocks (**10, 30**) befinden.

26. Verfahren gemäß Anspruch 25,

bei dem jedem Eintrag in den variablen Teil (**30**) ein Hüllenblock (**54**) vorausgeht, der einen demselben folgenden Eintrag und dessen Länge spezifiziert.

27. Verfahren zum Entschlüsseln von Multimediadaten, die nach Anspruch 1 verschlüsselt sind, mit folgenden Schritten:

Lesen des Bestimmungsdatenblocks (**10, 30**);

Auswählen eines Bestimmungsdaten-Entschlüsselungsalgorithmus aus einer Mehrzahl von Entschlüsselungsalgorithmen aufgrund des Bestimmungsdaten-Verschlüsselungsindex (**18**);

Auswählen eines Multimediadaten-Entschlüsselungsalgorithmus aus einer Mehrzahl von Entschlüsselungsalgorithmen aufgrund des Multimediadaten-Verschlüsselungsindex (**18**);

Entschlüsseln des verschlüsselten Abschnitts des Bestimmungsdatenblocks (**10, 30**) unter Verwendung des Bestimmungsdaten-Entschlüsselungsalgorithmus; und

Entschlüsseln des Multimediadatenblocks unter Verwendung des ausgewählten Multimediadaten-Entschlüsselungsalgorithmus, wobei der Schritt des Entschlüsselns des Multimediadatenblocks nur dann über eine vorbestimmte Zeitdauer hinaus fortgesetzt wird, wenn die Vorrichtung zum Entschlüsseln eine für den Freiindex (**42**) geeignete Einstellung aufweist, nach dem Hauptpatent 19625635.6-31

gekennzeichnet durch folgenden Schritt:

Empfangen der Pakete eines verschlüsselten Datenstroms und Entpacken derselben, um den Bestimmungsdatenblock (**10, 30**) und den Multimediadatenblock zu erhalten.

28. Verfahren nach Anspruch 27 zum Entschlüsseln von Multimediadaten, die nach Anspruch 1 bis 14 verschlüsselt sind,

bei dem lediglich der Anteil der Multimediadaten in dem Multimediadatenblock entschlüsselt wird, der

durch den Mengenindex (32) angezeigt ist.

29. Verfahren gemäß einem der Ansprüche 27 oder 28, zum Entschlüsseln von Multimediadaten, die nach einem der Ansprüche 1 bis 15 verschlüsselt sind, bei dem der Schritt des Entschlüsselns des Multimediadatenblocks nur dann durchgeführt wird, wenn ein Benutzer Produkte eines durch den Lieferantenindex (36) gekennzeichneten Lieferanten verwenden darf.

30. Verfahren gemäß einem der Ansprüche 27 bis 29 zum Entschlüsseln von Multimediadaten, die nach einem der Ansprüche 1 bis 16 verschlüsselt sind, bei dem der Schritt des Entschlüsselns des Multimediadatenblocks nur dann durchgeführt wird, wenn ein Benutzer bei dem durch den Großhändlerindex (36) bezeichneten Großhändler autorisiert ist, Produkte desselben zu verwenden.

31. Verfahren nach einem der Ansprüche 27 bis 30 zum Entschlüsseln von Multimediadaten, die nach Anspruch 17 verschlüsselt sind, bei dem der Schritt des Entschlüsseln des Multimediadatenblocks nur dann durchgeführt wird, wenn der durch den Benutzerindex (38) gekennzeichnete Benutzer die Multimediadaten entschlüsselt.

32. Verfahren gemäß Anspruch 27 bis 31 zum Entschlüsseln von Multimediadaten, die nach Anspruch 18 verschlüsselt sind, bei dem der Schritt des Entschlüsselns des Multimediadatenblocks das Berechnen eines für den ausgewählten Entschlüsselungsalgorithmus nötigen Entschlüsselungsschlüssel aufweist, der sich aus einer Kombination des Benutzerindex (38), des Herausforderungsindex (44) und des Antwortindex (46) ergibt.

33. Vorrichtung zum Verschlüsseln von Multimediadaten, um eine verschlüsselte Multimediadatei zu erhalten, die einen Bestimmungsdatenblock (10, 30) und einen Multimediadatenblock aufweist, mit folgenden Merkmalen:

einer Einrichtung zum Eintragen eines Bestimmungsdaten-Verschlüsselungsindex (18) in den Bestimmungsdatenblock (10, 30), wobei der Bestimmungsdaten-Verschlüsselungsindex (18) auf einen zum Verschlüsseln eines Abschnitts des Bestimmungsdatenblocks (10, 30) zu verwendenden Bestimmungsdaten-Verschlüsselungsalgorithmus hinweist;

einer Einrichtung zum Eintragen eines Multimediadaten-Verschlüsselungsindex (34, 36, 38, 44, 46) in den Bestimmungsdatenblock (10, 30), wobei der Multimediadaten-Verschlüsselungsindex (34, 36, 38, 44, 46) auf einen zum Verschlüsseln zumindest eines Anteils des Multimediadatenblocks zu verwendenden Multimediadaten-Verschlüsselungsalgorithmus hinweist;

einer Einrichtung zum Eintragen eines Freiindex (42) in den Bestimmungsdatenblock (10, 30), wobei der Freiindex (42) die Vorrichtung zum Entschlüsseln identifiziert, mit der ein Entschlüsseln der verschlüsselten Multimediadaten über eine vorbestimmte Zeitdauer hinaus möglich ist;

einer Einrichtung zum Auswählen des Bestimmungsdaten-Verschlüsselungsalgorithmus aus einer Mehrzahl von Verschlüsselungsalgorithmen aufgrund des Bestimmungsdaten-Verschlüsselungsindex (18);

einer Einrichtung zum Auswählen des Multimediadaten-Verschlüsselungsalgorithmus aus einer Mehrzahl von Verschlüsselungsalgorithmen aufgrund des Multimediadaten-Verschlüsselungsindex (34, 36, 38, 44, 46);

einer Einrichtung zum Verschlüsseln des Abschnitts des Bestimmungsdatenblocks (10, 30) mit dem Bestimmungsdaten-Verschlüsselungsalgorithmus, wobei der Abschnitt des Bestimmungsdatenblocks (10, 30) den Bestimmungsdaten-Verschlüsselungsindex nicht aufweist; und

einer Einrichtung zum zumindest teilweisen Verschlüsseln des Multimediadatenblocks mit dem Multimediadaten-Verschlüsselungsalgorithmus, nach dem Hauptpatent 19625635.6-31;

gekennzeichnet durch

eine Einrichtung zum Verpacken der Multimediadatei in ein Haupt-Bestimmungsdatenpaket, in ein Multimediadaten-Bestimmungsdatenpaket und in ein Multimediadatenpaket, um einen Datenstrom aus verschlüsselten Multimediadaten zu erzeugen, derart, daß

- das Haupt-Bestimmungsdatenpaket den Bestimmungsdaten-Verschlüsselungsindex des Bestimmungsdatenblocks (10, 30) aufweist,
- das Multimediadaten-Bestimmungsdatenpaket den Multimedia-Verschlüsselungsindex des Bestimmungsdatenblocks (10, 30) aufweist; und
- das Multimediadatenpaket zumindest einen Teil des Multimediadatenblocks aufweist.

34. Vorrichtung zum Verschlüsseln nach Anspruch 33, die ferner folgende Merkmale aufweist:

eine Einrichtung zum Eintragen eines Benutzerindex (38), der den Benutzer anzeigt, der die Multimediadaten benutzen kann, eines Herausforderungsindex (44) und eines Antwortindex (46) in einen Bestimmungsdatenblock (10, 30); und

eine Einrichtung zum Berechnen des Antwortindex (46) aus dem Benutzerindex (38), dem Herausforderungsindex (44) und einem für eine Verschlüsselungsvorrichtung spezifischen Schlüssels.

35. Vorrichtung zum Entschlüsseln von Multimediadaten, die nach Anspruch 1 verschlüsselt sind, mit folgenden Merkmalen:

einer Einrichtung zum Lesen des Bestimmungsdatenblocks (10, 30);

einer Einrichtung zum Auswählen eines Bestimmungsdaten-Entschlüsselungsalgorithmus aus einer Mehrzahl von Entschlüsselungsalgorithmen aufgrund des Bestimmungsdaten-Verschlüsselungsindex (18);

einer Einrichtung zum Auswählen eines Multimediadaten-Entschlüsselungsalgorithmus aus einer Mehrzahl von Entschlüsselungsalgorithmen aufgrund des Multimediadaten-Verschlüsselungsindex (18);

einer Einrichtung zum Entschlüsseln des verschlüsselten Abschnitts des Bestimmungsdatenblocks (10, 30) unter Verwendung des Bestimmungsdaten-Entschlüsselungsalgorithmus; und

einer Einrichtung zum Entschlüsseln des Multimediadatenblocks unter Verwendung des ausgewählten Multimediadaten-Entschlüsselungsalgorithmus, wobei die Vorrichtung zum Entschlüsseln der Multimediadaten nur dann über eine vorbestimmte Zeitdauer hinaus den Multimediadatenblock entschlüsselt, wenn die Vorrichtung eine für den Freiindex (42) geeignete Einstellung aufweist, nach dem Hauptpatent 19625635.6-31;

gekennzeichnet durch

eine Einrichtung zum Empfangen der Pakete eines verschlüsselten Datenstroms und zum Entpacken derselben, um den Bestimmungsdatenblock (10,30) und den Multimediadatenblock zu erhalten.

36. Vorrichtung zum Entschlüsseln nach Anspruch 35, die ferner eine Einrichtung zum Berechnen eines Schlüssels für den ausgewählten Multimediadaten-Entschlüsselungsalgorithmus aus einer Kombination eines in dem Bestimmungsdatenblock (10, 30) vorhandenen

Benutzerindex (38), eines in demselben vorhandenen Herausforderungsindex (44) und eines in demselben vorhandenen Antwortindex (46) aufweist.

Hierzu 3 Seite(n) Zeichnungen

Nummer: DE 197 44 293 C1
Int. Cl.[6]: H 04 L 9/32
Veröffentlichungstag: 1. Juli 1999

	NAME DES EINTRAGS	GRÖSSE	NAME DES UNTER-EINTRAGS	GRÖSSE	VER-SCLÜSS.?
12	DATENINDEX	4 BYTE	IDENTIFIZIERER	24 BYTE	NEIN
			VERSION	8 BYTE	
14	LÄNGENINDEX	4 BYTE	BESTIMMD.-BLOCKLÄNGE	32 BYTE	NEIN
16	VERSATZINDEX	4 BYTE	VERSATZ	32 BYTE	
18	VERSCHLÜSSE-LUNGSINDEX	4 BYTE	VERFAHREN	16 BYTE	NEIN
			SCHLÜSSEL	16 BYTE	
	VARIABLER TEIL DES BESTIMMUNGSDATENBLOCKS (SIEHE FIG.2)				
20	PRÜFSUMME	16 BYTE	MDS-FINGERABDRUCK	128 BYTE	JA

10

FIG.1

	ID	NAME DES EINTR.	GRÖSSE	NAME DES UNTER-EINTRAGS	GRÖSSE	VER-SCHLÜSS?
32	0 x 01	MENGENINDEX	8 BYTE	SCHRITT	16 BIT	NEIN
				MENGE	16 BIT	
34	0 x 02	LIEFERANTENINDEX	8 BYTE	LIEFERANT	32 BIT	NEIN
36	0 x 03	GROSSHÄNDLERIND.	8 BYTE	GROSSHÄNDLER	32 BIT	NEIN
38	0 x 04	BENUTZERINDEX	8 BYTE	BENUTZER	32 BIT	NEIN
40	0 x 05	FLAGINDEX	8 BYTE	GEHEIM	1 BIT	NEIN
				REGISTRIERUNG	1 BIT	
				HERAUSFORDERUNG	1 BIT	
42	0 x 06	FREIINDEX	20 BYTE	SERIENNUMMER	32 BIT	JA
				BENUTZERDATEN	96 BIT	
44	0 x 07	HERAUSFORDE-RUNGSINDEX	20 BYTE	DECODIERERTYP	4 BIT	JA
				CODIEREVERSION	4 BIT	
				DECOD.-ZUSTAND	8 BIT	
				GROSSHÄNDLERINDEX	32 BIT	
				BENUTZERINDEX	32 BIT	
				BENUTZERDATEN	46 BIT	
46	0 x 08	ANTWORTINDEX	20 BYTE	ANTWORTINDEX	128 BIT	
48	0 x 09	AUSLAUFINDEX	8 BYTE	AUSLAUFDATUM	32 BIT	NEIN
50	0 x 0a	MULTIMEDIA-INDEX	16 BYTE	LANDCODE	16 BIT	
				EIGENTÜMERCODE	24 BIT	
				JAHR	16 BIT	
				BEZEICHNUNGSCODE	40 BIT	
52	0 x 0b	BENUTZERCODE-INDEX	16 BYTE	BENUTZERCODE	32 BIT	NEIN

30

FIG.2

Nummer: DE 197 44 293 C1
Int. Cl.[6]: H 04 L 9/32
Veröffentlichungstag: 1. Juli 1999

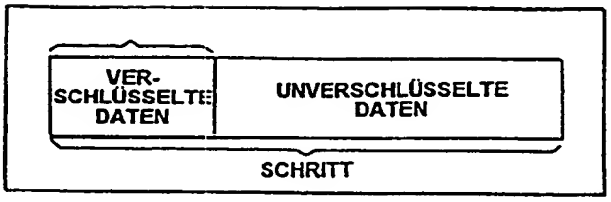

FIG.3

54

NAME DES EINTRAGS:	GRÖSSE	NAME DES UNTEREINTRAGS		VER-SCHLÜSS.?
EINTRAG	4 BYTE	EINTRAGSIDENTIFIKATION EINTRAGSLÄNGE		NEIN

FIG.4

Nummer: DE 197 44 293 C1
Int. Cl.[6]: H 04 L 9/32
Veröffentlichungstag: 1. Juli 1999

	MENGENINDEX 32	LIEFERANTENINDEX 34	GROSSHÄNDLER-INDEX 36	BENUTZERINDEX 38	FREIINDEX 42	HERAUFORDERUNGS-INDEX 44	ANTWORTINDEX 46	AUSLAUFDATUM 48
UNVERSCHÜSSELTER BITSTROM								
VERSCHLÜSSELTER BITSTROM MIT DEMOSPIELER (FREISCHALTUNG)	X				X			
VERSCHLÜSSELTER BITSTROM FÜR BENUTZER EINES SPEZIFISCHEN GROSSHÄNDLERS (DEMOSPIELER FREISCHALTUNG)	X		X		X			
VERSCHLÜSSELTER BITSTROM FÜR ALLE BENUTZER EINES SPEZIFISCHEN LIEFERANTEN	X	X	X					(X)
VERSCHLÜSSELTER BITSTROM FÜR EINEN BENUTZER EINES SPEZIFISCHEN LIEFERANTEN	X	X	X	X				(X)
VERSCHLÜSSELTER BITSTROM FÜR EINEN BENUTZER EINES SPEZIFISCHEN LIEFERANTEN (SCHNELLERER DATENBANKZUGRIFF)	X	X	X	X		X	X	(X)

FIG.5